Release Notes for Cisco Catalyst 8000V Edge Software, Cisco IOS XE 17.16.x

First Published: 2024-12-22

Full Cisco Trademarks with Software License

Cisco Catalyst 8000V Edge Software Overview

About Cisco Catalyst 8000V

Cisco Catalyst 8000V Edge Software or Cisco Catalyst 8000V is a software-based, virtual router that combines the functionalities of Cisco Cloud Services Router (Cisco CSR1000V) and Cisco Integrated Services Virtual Router (Cisco ISRv) into a single image that is intended for deployment in on-prem branches, data centers, colocation data centers, and public clouds.

Cisco Catalyst 8000V supports NIM modules on Cisco ENCS platforms, runs on any x86 platform, and is supported on ESXi, KVM, and Cisco NFVIS hypervisors. Further, you can deploy this router on public cloud providers such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and Alibaba Cloud.

When you deploy Cisco Catalyst 8000V as a VM, the Cisco IOS XE software behaves similar to a traditional Cisco router (hardware platform). You can configure different features depending on the Cisco IOS XE software version.

Features

- **Hardware independence**: The Cisco Catalyst 8000V router uses the benefits of virtualization in the cloud to provide hardware independence. Since the Cisco Catalyst 8000V runs as a virtual machine, you can use this router on any x86 hardware that the virtualization platform supports.
- **Sharing of host hardware resources**: The host server hardware resources such as CPU cores, memory, and disk are managed by the hypervisor, and these resources are shared among the guest VMs. You can regulate the amount of hardware resources assigned to a specific Cisco Catalyst 8000V VM instance.
- **Flexibility in deployment**: You can easily move a VM from one server to another. Thus, you can move a Cisco Catalyst 8000V instance from a server in one physical location to a server in another physical location without moving any hardware resources.
- **Enhanced software security - Secure Object Store**: In Cisco Catalyst 8000V, storage partitions for NVRAM, licensing, and other data are created as object stores. The individual object stores are encrypted to ensure data security, and this product is Cisco Secure Development life cycle (CSDL) compliant. Further, Cisco Catalyst 8000V supports a 16G disk profile.

Hardware Requirements

For hardware requirements and installation instructions, see the Cisco Catalyst 8000V Edge Software Installation And Configuration Guide.

Software Images and Licenses

The following sections describe the licensing and software images for Cisco Catalyst 8000V.

Cisco Catalyst 8000V Software Licenses

The Cisco Catalyst 8000V is licensed based on throughput, feature-set, and the licensing term. This product supports Cisco Smart Licensing Usage Policy as well as Cisco DNA Licensing. Based on whether you want to opt for purchased licenses that go with the Cisco Catalyst 8000V instance, or a subscription-based license, choose one of the following options:

Subscription-Based Licensing via Cisco DNA

You can purchase a subscription license for Cisco Catalyst 8000V through the following licenses that are available via Cisco DNA:

- Cisco Catalyst 8000V - Network-Advantage
- Cisco Catalyst 8000V - Network-Essentials

For more information on Cisco Catalyst 8000V DNA licensing, see Cisco DNA Software for SD-Wan and Routing Ordering Guide.

Bring-Your-Own-Licensing

You also have an option to purchase and use licenses with Cisco Catalyst 8000V as a Bring-Your-Own-License (BYOL) instance or as a Pay-As-You-Go (PAYG) instance.

To use a Cisco Catalyst 8000V - BYOL license, see Licenses and Licensing Models to know to how install and configure your license.

If you have upgraded to Cisco Catalyst 8000V from a Cisco CSR 1000V or a Cisco ISRV, you must use Smart Licensing Using Policy (SLP). Traditional licenses do not work after the upgrade.

Pay-As-You-Go Licensing

Cisco Catalyst 8000V supports the PAYG Licensing model with Amazon Web Services (AWS) and Microsoft Azure Marketplace. Cisco Catalyst 8000V hourly-billed AMI or Pay As You Go licensing model allows you to consume an instance for a defined period of time. In this licensing model, you can directly launch the instance from the AWS or Azure Marketplace and start using the instances. The licenses are embedded in the image.

Note For demo or evaluation licenses, contact your Cisco Account Team if you have a direct purchase agreement with Cisco, or your Cisco Partner or Reseller.

For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.

Software Image Nomenclature for Installation Files

The Cisco Catalyst 8000V installation file nomenclature indicates properties supported by the router in a given release.

For example, these are filename examples for the Cisco IOS XE 17.16.1a release:

- c8000v-universalk9.17.16.01a.ova

- c8000v-universalk9.17.16.01a.iso
- c8000v-universalk9.17.16.01a.qcow2

The following table lists the filename attributes along with its properties:

Table 1: Installation Filename Attributes

Filename Attribute	Properties
universalk9	Specifies the package that you are installing. Images with the universalk9 designation in the image name refers to a universal image that offers all the Cisco IOS features including strong payload cryptography features such as IPSec VPN, SSL VPN, and Secure Unified Communications. This image also supports security features like Zone-Based Firewall and intrusion prevention.
17.16.01a	Indicates that the software image is mapped to the Cisco IOS XE 17.16.1a release.

Product Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround or other user action. For more information, see https://www.cisco.com/c/en/us/support/web/field-notice-overview.html.

We recommend that you review the field notices to determine whether your software or hardware platforms are affected. You can access the field notices from https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html#%7Etab-product-categories.

New and Enhanced Features for Cisco IOS XE 17.16.x

New and Enhanced Software Features in Cisco IOS XE 17.16.1a

Note Cisco IOS XE 17.16.1a is the first release for Cisco Catalyst 8000V in the Cisco IOS XE 17.16.x release series.

Table 2: Software features

Feature	Description
Configure Source Interface for High Speed Logging	From Cisco IOS XE 17.16.1a, you can configure source interfaces for High-Speed Logging (HSL) and SysLog for security logging in Cisco SD-WAN Manager. You can also enable HSL for your firewall messages, to allow a firewall to log records with minimum impact to packet processing.
Disablement of Weak SSH Algorithms	From Cisco IOS XE 17.16.1a, the ssh-rsa algorithm is disabled by default on port 22 to improve security.
Enhanced Support for Binary Tracing	From Cisco IOS XE 17.16.1a onwards, you can retrieve events sent to the IOS process in the binary trace using the **show logging process IOS module nhrp** command, without enabling DMVPN event tracing.
Enhancement to the **show cellular 0/x/0 connection** Command	From Cisco IOS XE 17.16.1a, the output for the **show cellular 0/x/0 connection** command includes the following parameters: • Access Point Name (APN), and • Cellular Link Uptime
Enhancements to Segment Routing over IPv6 Dataplane	From Cisco IOS XE 17.16.1a, Segment Routing over IPv6 dataplane supports these functionalities: • eBGP Inter-AS • PCE-Delegated Path Computation • Enhancements to OAM Traffic Engineering
Improved Workflow to Configure Branch Connect Solution	This release introduces a simplified guided workflow to ease each step of configuring site to cloud connectivity.
Monitoring Application Performance on SD-Routing Devices	In Cisco IOS XE 17.16.1a, you can now monitor TCP and RTP traffic on DMVPN tunnels for IKEv2 traffic using Application Response Time (ART) monitor and Media monitor respectively. This functionality is only supported on DMVPN tunnels with IKEv2 encryption.

Feature	Description
Monitoring Crypto VPN Solutions on SD-Routing Devices	If you have configured crypto VPN solutions such as DMVPN, FlexVPN or Layer 3 VPNs on SD-Routing devices, you can use Cisco Catalyst SD-WAN Manager to visualize the VPN solution deployed in the network and observe the functioning of the devices using various states, stats, charts and events. Having high visibility into the network can help identify errors in real time therefore reducing the network downtime.
Speed Test Enhancement for SD-Routing Devices	From Cisco IOS XE 17.16.1a, Cisco Catalyst SD-WAN Manager enables site-to-site speed tests to measure bandwidth between devices over DMVPN tunnels. These tests check upload speed from the source device to the destination, and measure download speed from destination to the source device.
Support for Enrollment over Secure Transport (EST)	From Cisco IOS XE 17.16.1a onwards, you can use HTTP-based authentication for EST Client Support, using the **enrollment http username [http_username] password [http_password]** command.
UTD Container Management for SD-Routing Devices	When Cisco IOS-XE autonomous devices transition to Cisco SD-Routing mode, the Unified Threat Defense (UTD) Container Migration feature ensures that existing container functionalities are preserved. From Cisco IOS XE 17.16.1a you can detect, upgrade, and manage UTD Security Virtual Images through Cisco Catalyst SD-WAN Manager. For devices without pre-existing containers, you can also install and manage UTD images using policy groups.

Table 3: Cisco Unified Border Element (CUBE) features

Feature	Description
CUBE: Secure Communications Interoperability Protocol (SCIP) support in CUBE	From Cisco IOS XE 17.16.1a onwards, support for Secure Communication Interoperability Protocol (SCIP) voice and video codec is available, that ensures secure traffic sessions between the endpoints. **Note** Preview Feature Disclaimer: The Secure Communications Interoperability Protocol (SCIP) feature in Cisco IOS XE 17.16.1a release is available in 'preview' mode as it includes limited functionality or incomplete software dependencies. Cisco reserves the right to disable preview features at any time without notice. Cisco Technical Support provides reasonable effort support for features in preview mode. There is no Service Level Objective (SLO) in response times for features in preview mode; response times may be slow.

Resolved and Open Bugs - Cisco IOS XE 17.16.x

Resolved Bugs - Cisco IOS XE 17.16.1a

Identifier	Headline
CSCwn07540	C8000v crashed due to IOSXE_INFRA-2-FATAL_NO_PUNT_KEEPALIVE.
CSCwm56800	FIA trace packet decode displays incorrect value for fragmentation offset.
CSCwk78018	SD-ROUTING: Yang model does not handle properly default ikev2 authorisation policy.
CSCwm67178	Cannot configure MD5 for the hash under the ikev2 proposal when compliance shield is disabled.
CSCwk42493	Cellular interface in last-resort mode should be admin up, line protocol down.
CSCwk62954	Multiple "match address local interface <int>" not pushed under crypto profile.
CSCwk79606	PKI trustpoint password command only allows encryption type 0 and 7 on all IOS XE platforms.
CSCwj33723	Config not synced between active and 3rd member of stack.
CSCwm48459	Software crash with critical process vip_confd_startup_sh fault on rp_0_0 (rc=6).
CSCwm50619	Data policy commit failure occurs when export-spread is enabled in Cflowd configuration.

Identifier	Headline
CSCwn29062	Traceback log output with "DATACORRUPTION" error logs.
CSCwm62981	Device crashes with PKI "revocation-check ocsp none" enabled.
CSCwm70520	LNS tracebacks generation.
CSCwm74317	Syslog message '%CRYPTO_ENGINE-4-CSDL_COMPLIANCE_RSA_WEAK_KEYS: RSA keypair CISCO_IDEVID_CMCA_SUDI.
CSCwm54978	Selinux: Subject polaris_iosd_t denials 2024-09-16 06:43:22.
CSCwm77426	Unexpected reload in NHRP, cache freed prior to function call.

Open Bugs - Cisco IOS XE 17.16.1a

Identifier	Headline
CSCwn09185	Traffic loss observed on minimal values with time based policy-map.
CSCwn26353	BFD sessions via TLOC-Ext do not come up when IPv6 is dynamically changed.
CSCwn40906	Router crash observed when optimizing encrypted traffic with DRE.
CSCwm71639	cpp_cp_svr crash noticed when configured service-policy to a dialer interface.
CSCwm73195	C8000V 'show interfaces' counters are incorrect and unreasonably large.
CSCwn02485	Fragmented UDP SIP packets dropped on PE with IpFragErr on IP VFR and MPLS enabled tunnel interface.
CSCwn24226	GETVPN mismatch in GMs reported across COOP due to KEK sync issue between primary & secondary KSs.
CSCwn34457	Post power cycle, unable to login to router due to error authentication failed.
CSCwn19586	Certificate-based MACsec flapping when dot1x reauth timers are set and after reload.
CSCwk20995	PPPoE session with sub-interface getting stuck after reboot.
CSCwm87270	MKA session down with "ICV Verification of a MKPDU failed for" error on one of the interfaces.
CSCwn39447	Speed test might work abnormally after changing system-ip.
CSCwm43089	Low throughput with C8000v.
CSCwm71868	Stopping C8000v in Azure results in device reload, then stop after 10 minutes.
CSCwn35476	cflowd source interface for sub-interface does not get pushed.
CSCwm28388	Traceback seen - EVENTLIB-3-CPUHOG - fman_fp_image.

Identifier	Headline
CSCwo39530	Applied changes in the filter of pcap fileds are not reflecting after refreshing.

Related Documentation

Cisco Catalyst 8000V Edge Software Product Page

Cisco Catalyst 8000V Edge Software Data Sheet

Cisco Catalyst 8000V Edge Software Installation And Configuration Guide

Cisco Catalyst 8000V Edge Software High Availability Configuration Guide

Troubleshooting Guide for Cisco Catalyst 8000V Edge Software

Smart Licensing Using Policy for Cisco Enterprise Routing Platforms

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at https://www.cisco.com/en/US/support/index.html.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.